

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED  
LODGEDENTERED  
RECEIVED

DEC -1 2016

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

BY DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)Certain student.angelina.edu email accounts, et al.,  
stored at premises controlled by Google, Inc.

Case No.

MT16-504

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 1028A	Aggravated Identity Theft
Title 18, U.S.C. § 1029	Access Device Fraud
Title 18, U.S.C. § 1030	Computer Fraud

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

STACY MULDOON, SPECIAL AGENT FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Dec. 1, 2016

Judge's signature

City and state: SEATTLE, WASHINGTON

MARY ALICE THEILER U.S. MAGISTRATE JUDGE

Printed name and title

2016R01051



- <https://drive.google.com/uc?export=download&id=0B-21sH2hZMoZMFluQlFoeTR0v0k>
- [https://drive.google.com/uc?export=download&id=0B\\_MZgxQt5pYfWUFudU5kcDIOSXM](https://drive.google.com/uc?export=download&id=0B_MZgxQt5pYfWUFudU5kcDIOSXM)
- [https://drive.google.com/file/d/0B\\_MZgxQt5pYfVfFo1RVhSdGwxRW8/view?usp=sharing](https://drive.google.com/file/d/0B_MZgxQt5pYfVfFo1RVhSdGwxRW8/view?usp=sharing)
- [https://drive.google.com/a/student.angelina.edu/file/d/0B\\_MZgxQt5pYfVfFo1RVhSdGwxRW8/view?usp=sharing\\_eid&ts=577af79f](https://drive.google.com/a/student.angelina.edu/file/d/0B_MZgxQt5pYfVfFo1RVhSdGwxRW8/view?usp=sharing_eid&ts=577af79f)

(hereinafter, "the SUBJECT GOOGLE DRIVE ACCOUNTS"). The accounts to be searched are described further in the following paragraphs and in Attachment A.

3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1029 (Access Device Fraud); 18 U.S.C. § 1030 (Computer Fraud); 18 U.S.C. § 1349 (Conspiracy to Commit Bank and Wire Fraud) have been committed by unknown persons. There is also probable cause to search the information described in

1 Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further  
2 described in Attachment B.

### 3 SUMMARY OF PROBABLE CAUSE

4 6. The FBI is investigating a malware scheme that seeks, among other things, to  
5 steal personal and financial information. The malware scheme has used its malicious  
6 software to compromise the computer systems of Eddie Bauer and other companies across  
7 the country.

8 7. On November 3, 2016, the Court issued search and seizure warrants for the  
9 SUBJECT EMAIL ACCOUNTS. The affidavit made in support of the search warrant  
10 application for those warrants is attached and incorporated herein by reference. In summary,  
11 the perpetrators of the malware scheme fraudulently set up three student email accounts at  
12 Angelina College and used one or more of those accounts to send phishing emails to Eddie  
13 Bauer and other businesses. The emails contained attachments or links to documents that  
14 when opened and fully enabled would allow malware to be downloaded onto the victims'  
15 computers. It appears that the central purpose of this malicious code is to capture and export  
16 financial information belonging to the victims' customers.

17 8. In response to the search warrants, Angelina College provided, *inter alia*,  
18 emails contained in the SUBJECT EMAIL ACCOUNTS. Over 6,000 emails were found in  
19 the SUBJECT EMAIL ACCOUNTS, and a high percentage of those emails appear to be  
20 emails that the malware scheme sent to victims in an attempt to compromise the victims'  
21 systems with malware. Many of the emails attached suspected malicious Word documents,  
22 similar to the Word attachment that scheme to use to attempt to compromise Eddie Bauer's  
23 computer system. Analysis of these documents by the FBI is pending.

24 9. A small number of these emails contained links to files hosted by Google in  
25 their "Google Drive" service. Based on a comparison of the contents of the text of these  
26 emails to those emails containing known or suspected malicious attachments, I believe that  
27 the files hosted at Google Drive and referenced in these emails are malicious and are  
28 intended to compromise the computer systems of the recipients of these emails.

1        10. For example, in an email sent on May 10, 2016, the user of email account  
2 149wlong@student.angelina.edu sent an email to oc2015@ocharleys.com. This email  
3 contained text saying that the included Google Drive link was associated with initial pre-  
4 order information and requested a confirmation of booking. The Google Drive link was  
5 <https://drive.google.com/uc?export=download&id=0B-21sH2hZMoZMFluQlFoeTR0v0k>.  
6 This was one of approximately twenty reservation-related emails sent out by  
7 149wlong@student.angelina.edu between May 9, 2016 and May 10, 2016.

8        11. O'Charley's is a restaurant brand owned by American Blue Ribbon Holdings  
9 (ABRH). ABRH was the victim of an intrusion similar to that experienced by Eddie Bauer  
10 in which credit card data was targeted and stolen. In another reservation-related email also  
11 sent on May 10, 2016 by 149wlong@student.angelina.edu to the O'Charley's email account,  
12 the sender of the email included a link to the exact same Google Drive document. Based on  
13 this file being sent to two likely distinct O'Charley's restaurant locations, I do not believe  
14 that the linked document is a legitimate reservation request.

15        12. Similarly, in an email sent by 349abounds@student.angelina.edu on May 19,  
16 2016 to customer.success@pfsbrands.com, the sender included the following link to a  
17 Google Drive document:  
18 [https://drive.google.com/uc?export=download&id=0B\\_MZgxQt5pYfWUFudU5kcDIOSXM](https://drive.google.com/uc?export=download&id=0B_MZgxQt5pYfWUFudU5kcDIOSXM).  
19 This link was included in an email referencing a purported experience at one of the  
20 recipient's locations. According to their website, PFSbrands is the parent company for  
21 Champs Chicken and Cooper's Express which are both franchised fried chicken restaurant  
22 brands. In an email sent by 349abounds@student.angelina.edu on May 19, 2016 to  
23 barkley.carr@pfsbrands.com approximately twenty minutes after the prior email, the sender  
24 included the same link to a Google Drive document as sent to  
25 customer.success@pfsbrands.com. This was included in a message in which the sender  
26 thanked Barkley Carr for the "instant reply." I believe that this was in response to an  
27 unrecovered email from PSFbrands to 349abounds@student.angelina.edu.

1           13.     There is some indication that perpetrator(s) of the malware scheme used at  
2 least one of the SUBJECT EMAIL ACCOUNTS to communicate with potential co-  
3 conspirators or to forward information to another account used by the scheme serviced by the  
4 company YOPMail. According to YOPmail's website, YOPMail offers disposable and free  
5 email addresses and stands for "Your Own Protection Mail." The site offers email addresses  
6 that require no registration and does not require a password to access a specific inbox. It also  
7 offers the ability to forward email from one YOPMail account to another, and will generate a  
8 random Yopmail email address if a user so chooses. The site advertises that messages are  
9 only kept for 8 days. To prevent abuse, YOPMail accounts cannot be used to send email to  
10 another address unless that address is also a YOPMail account. YOPMail supports multiple  
11 domains.

12           a.     In an email sent by 349abounds@student.angelina.edu to  
13 besogonn@yopmail.com on July 4, 2016, the writer of the email sent a notification to  
14 besogonn@yopmail.com informing the recipient that the sender was sharing a Google Drive  
15 document with the recipient. The Google Drive document was located at  
16 [https://drive.google.com/a/student.angelina.edu/file/d/0B\\_](https://drive.google.com/a/student.angelina.edu/file/d/0B_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing_eid&ts=577af79f)  
17 [MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing\\_eid&ts=577af79f](https://drive.google.com/a/student.angelina.edu/file/d/0B_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing_eid&ts=577af79f). There was no  
18 additional text describing the document or attempting to entice the recipient to open it.

19           b.     In an email sent by 349abounds@student.angelina.edu to  
20 besogonn@yopmail.com on July 5, 2016, the writer of the email again sent a link to  
21 besogonn@yopmail.com with a link to the same Google Drive document as was sent on July  
22 4, 2016. This email differed from the previous email in that the link was "plain text" and not  
23 a formatted notification sent by Google Drive itself on behalf of  
24 349abounds@student.angelina.edu. The link was to  
25 [https://drive.google.com/file/d/0B\\_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing](https://drive.google.com/file/d/0B_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing).  
26 I believe that, while the link differs slightly in terms of parameters, it points to the same  
27 document based on the string "0B\_MZgxQt5pYfVFo1RVhSdGwxRW8" remaining the  
28 same in both links.



1 c. Both emails contained no enticing text or additional content. Based on training  
2 and experience and the nature of the communication, I believe that the sender of this email  
3 was sharing the file with the unidentified recipient. As there was no text to try and entice the  
4 recipient to open the email or explain the linked document it is possible that the sender was  
5 sharing the file with a potential co-conspirator and/or themselves.

6 14. The FBI is reviewing approximately 6,000 emails provided to the FBI by  
7 Angelina College personnel pursuant to the previously granted search warrants for  
8 SUBJECT EMAIL ACCOUNTS. The FBI has found phishing emails in each of the  
9 SUBJECT EMAIL ACCOUNTS. The vast majority of the emails in the SUBJECT  
10 ACCOUNTS appear to fall into one of several categories: initial or follow-up "phishing"  
11 emails to individuals or organizations that the malware scheme is attempting to compromise;  
12 email notifications that previous "phishing" emails were opened, transmitted, or  
13 undeliverable; email notifications by Google that the account had been accessed by a specific  
14 browser from a geographic location (ex. City, state, Country, Time Zone); or emails  
15 involving a specific legitimate online freelance hiring service called Upwork that the FBI  
16 believes the malware scheme used to hire freelancers to translate documents, generate email  
17 lists, or other similar activities to facilitate the malware scheme's phishing attempts. In  
18 selected cases, the users of SUBJECT EMAIL ACCOUNTS appear to have communicated  
19 directly with these freelancers via email, while in other cases the communication was sent  
20 via Upwork itself to and from the freelancers.

21  
22 **THE SUBJECT EMAIL GOOGLE DRIVE ACCOUNTS**  
23 **ARE PERMEATED WITH FRAUD**

24 15. As explained in the prior affidavit, the SUBJECT EMAIL ACCOUNTS were  
25 designed to facilitate the malware scheme and to create the illusion that the accounts  
26 belonged to actual students at Angelina college. The Walter Long account was an  
27 instrumentality of the computer intrusion. In two separate computer intrusions, the account  
28 was used to convey a fraudulent consumer complaint that attached additional malware. And,

1 employees at Angelina College report that they have connected the other two SUBJECT  
2 EMAIL ACCOUNTS (349abounds@student.angelina.edu and  
3 514hestes@student.angelina.edu) to additional fraudulent activity. The FBI's preliminary  
4 review of the emails contained in the SUBJECT ACCOUNTS indicate that one or more of  
5 the accounts were used to send thousands of phishing emails to victims designed to infect the  
6 victims' computer systems.

7 16. In addition, the FBI's preliminary review indicates that the SUBJECT  
8 GOOGLE DRIVE ACCOUNTS were used to facilitate the malware scheme. As explained  
9 above, there is probable cause to believe that the linked Google Drive documents were  
10 designed to operate in a manner similar to the Microsoft Word attachments used in the other  
11 phishing emails. That is, the victims opening and enabling of the linked documents would  
12 lead to the compromise of the victims' computer systems.

### 13 **BACKGROUND REGARDING GOOGLE'S SERVICES**

14 17. In my training and experience and according to information provided by  
15 Angelina College to the FBI, I have learned that Angelina College provides electronic mail  
16 ("e-mail") access to students at Angelina College. Angelina College allows students to  
17 obtain e-mail accounts at the domain name @student.angelina.edu, like the e-mail accounts  
18 listed in Attachment A. Faculty and staff at Angelina College are provided email addresses  
19 from a different domain.

20 18. According to Angelina College and publically available information, email for  
21 students at Angelina College is maintained and operated by Google, Inc. While email is  
22 minted and operated by Google Inc., personnel from Angelina College have access to the  
23 information sought by the prior search warrants, including IP login information and the  
24 contents of the accounts themselves. However, Angelina College has indicated that it does  
25 not have access to any other data associated with the SUBJECT EMAIL ACCOUNTS such  
26 as data that would be contained in an associated Google Drive account.

27 19. As Angelina College is not certain how the individual(s) created the subject  
28 accounts, the exact amount of subscriber information is unknown. However, subscriber



1 information for an Angelina College account would, based on my training and experience  
2 and information provided by Angelina College, be maintained by Google, Inc., on behalf of  
3 the college but would be accessible to college representatives.

4       20. E-mail providers like Google, Inc. typically retain certain transactional  
5 information about the creation and use of each account on their systems. This information  
6 can include the date on which the account was created, the length of service, records of log-  
7 in (i.e., session) times and durations, the types of service utilized, the status of the account  
8 (including whether the account is inactive or closed), the methods used to connect to the  
9 account (such as logging into the account via a website), and other log files that reflect usage  
10 of the account. In addition, e-mail providers often have records of the Internet Protocol  
11 address ("IP address") used to register the account and the IP addresses associated with  
12 particular logins to the account. Because every device that connects to the Internet must use  
13 an IP address, IP address information can help to identify which computers or other devices  
14 were used to access the e-mail account, which can help establish the individual or individuals  
15 who had dominion and control over the account

16       21. In general, an e-mail that is sent to an Angelina College or Google subscriber  
17 is stored in the subscriber's "mail box" on Google, Inc.'s servers until the subscriber deletes  
18 the e-mail. If the subscriber does not delete the message, the message can remain on Google,  
19 Inc.'s servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be  
20 available on Google, Inc.'s servers for a certain period of time.

21       22. When the subscriber sends an e-mail, it is initiated at the user's computer,  
22 transferred via the Internet to Google, Inc.'s servers, and then transmitted to its end  
23 destination. Google, Inc., on behalf of Angelina College, often maintains a copy of the e-  
24 mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Google, Inc.'s  
25 server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-  
26 mail, it may continue to be available on Google, Inc.'s servers for a certain period of time.

27       23. A sent or received e-mail typically includes the content of the message, source  
28 and destination addresses, the date and time at which the e-mail was sent, and the size and

1 length of the e-mail. If an e-mail user writes a draft message but does not send it, that  
2 message may also be saved by Google, Inc. but may not include all of these categories of  
3 data.

4 24. Google, Inc. provides a variety of online, or "cloud," services in addition to  
5 email access, to the public and to customers who utilize .edu accounts that are served by  
6 Google, Inc. Google's various cloud services are associated with a single Google account,  
7 which is typically associated with a Google email address, but can be associated with any  
8 email address. The various cloud services provided by Google, Inc. are optional, and can be  
9 turned "on" or "off" by the user.

10 25. In providing services such as Google Drive, Google Hangouts, calendar  
11 services, online file storage, storage of browsing history, storage of search history, and  
12 locations history, Google, Inc. collects information that constitute evidence of the crimes  
13 under investigation. For example, such evidence can be used to discover or confirm the  
14 identity and location users of the service at a particular time.

15 26. Google, Inc. is also able to provide information that will assist law  
16 enforcement in identifying other accounts associated with the subject accounts. In particular,  
17 Google, Inc. can provide information identifying and relating to other accounts used by the  
18 same subscriber. This information includes any forwarding or fetching accounts<sup>1</sup> related to  
19 the subject accounts; all other Google accounts linked to the subject accounts because they  
20 were accessed from the same computer (referred to as "cookie overlap"); all other Google  
21 accounts that list the same SMS phone number<sup>2</sup> as the subject accounts; all other Google

---

23 <sup>1</sup> A forwarding or fetching account related to one of subject accounts would be a separate  
24 email account that can be setup by the user to receive copies of all of the email sent to the  
25 subject account.

26 <sup>2</sup> The SMS phone number of a Google account is used by Google as an additional security  
27 precaution to verify the identity of the user by sending a text message with a code that must  
28 be entered in addition to the password to log into the account. This ensures that only a  
person with both the password and the phone tied to the SMS phone number can make  
changes to the account.

accounts that list the same recovery email addresses as the subject accounts; and all other Google accounts that share the same creation IP addresses<sup>3</sup> as the subject accounts. This information will assist law information in determine who controls the subject accounts and in identifying other accounts utilized by the malware scheme.

### PAST EFFORTS TO OBTAIN THIS EVIDENCE

27. On October 5, 2016, an FBI agent sent a preservation letter to Angelina College requesting that they preserve all evidence related to the account, 149wlong@student.angelina.edu, under authority of Title 18, United States Code, Section 2703(f)(1), for a period of 90 days. In a conversation with representatives from Angelina College on October 17, 2016, they stated they had voluntarily preserved the accounts 349abounds@student.angelina.edu and 514hestes@student.angelina.edu. This preservation was not requested by the FBI.

28. As the individual(s) utilizing these accounts are unknown to the FBI and to Angelina College, there has been no opportunity to obtain the emails sought by this search warrant via a search of the individual's computers or any other system.

29. Pursuant to a previously granted search warrant, Angelina College provided selected information to the FBI regarding the SUBJECT EMAIL ACCOUNTS. This included the contents of the SUBJECT EMAIL ACCOUNTS as well as limited login history for the accounts. No Google Drive data was provided pursuant to this prior search warrant, and Angelina College personnel informed the FBI that it is possible additional information may be maintained by and available only to Google, Inc. personnel.

30. A preservation letter was sent to Google, Inc. for the subject accounts on November 23, 2016. The associated Google reference number for the preservation request is 863881.

---

<sup>3</sup> The creation IP address is the IP address from which the Google account was created.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

31. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit Google, Inc., and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to Google, Inc. with directions that it identify the accounts described in Attachment A to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachment B to this affidavit.

32. The search warrant will direct Google, Inc. to create an exact copy of the specified accounts and records.

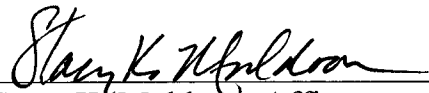
33. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

34. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.


35. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of e-mail communications, chat logs and documents, that identify any users of the subject account and e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

### CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

  
 Stacy K. Muldoon, Affiant  
 Special Agent  
 Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 1 day of December 2016.

  
 MARY ALICE THEILER  
 United States Magistrate Judge

**ATTACHMENT A**

**Account/s to be Searched**

This warrant applies to information contained in, related to, and associated with the following Google Inc./Google Payments Corporation ("Google") accounts, that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California:

1. 149wlong@student.angelina.edu;
2. 349abounds@student.angelina.edu;
3. 514hestes@student.angelina.edu; and
4. The Google Drive accounts associated with the following links:
  - <https://drive.google.com/uc?export=download&id=0B-21sH2hZMoZMFluQlFoeTR0v0k>
  - [https://drive.google.com/uc?export=download&id=0B\\_MZgxQt5pYfWUFudU5kcDIOSXM](https://drive.google.com/uc?export=download&id=0B_MZgxQt5pYfWUFudU5kcDIOSXM)
  - [https://drive.google.com/file/d/0B\\_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing](https://drive.google.com/file/d/0B_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing)
  - [https://drive.google.com/a/student.angelina.edu/file/d/0B\\_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing\\_eid&ts=577af79f](https://drive.google.com/a/student.angelina.edu/file/d/0B_MZgxQt5pYfVFo1RVhSdGwxRW8/view?usp=sharing_eid&ts=577af79f)



**ATTACHMENT B**

**I. Section I - Information to be disclosed by Google, for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized, and content, account records, and usage relating to those services;

d. All records or other information stored at any time by an individual using the account, including address books, calendars, pictures, location history, web history, search history, profile records, and contact and buddy lists;

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

In addition, Google shall identify and provide subscriber records and IP logs, excluding content, for any Google account associated with any forwarding or fetching accounts of the accounts listed in Attachment A, all other Google accounts linked to the accounts listed in Attachment A because of cookie overlap, all other Google accounts that

1 list the same SMS phone number as the accounts listed in Attachment A, all other Google  
 2 accounts that list the same recovery email address as the accounts listed in Attachment A,  
 3 and all other Google accounts that share the same creation IP address as the accounts listed  
 4 in Attachment A.

5 Please note that requests for preservation have been made by Angelina College and by  
 6 the FBI (#863881).

## 8 **II. Section II - Information to be seized by the government**

9 All information described above in Section I that constitutes fruits, contraband,  
 10 evidence and instrumentalities of violations of 18 U.S.C. § 1028A (Aggravated Identity  
 11 Theft), 18 U.S.C. § 1029 (Access Device Fraud); 18 U.S.C. § 1030 (Computer Fraud); and  
 12 18 U.S.C. § 1349 (Conspiracy to Commit Bank and Wire Fraud); from January 2016 to the  
 13 present, for each account or identifier listed on Attachment A, including the following:

14 a. Content that serves to identify any person who uses or accesses the  
 15 specified accounts or who exercises in any way any dominion or control over the accounts;

16 b. Content relating to planned, attempted, or successful breaches of or  
 17 intrusions into victims' computers or networks;

18 c. Content relating to the creation, acquisition, transfer, sharing, or sale of  
 19 malicious software;

20 d. Content relating to the acquisition, transfer, sharing, sale, or disposal of  
 21 servers, email accounts, or other web services accounts used by the person or persons  
 22 conducting intrusions or breaches;

23 e. Content relating to the acquisition, transfer, distribution, sharing or sale  
 24 of stolen credit card, debit card, gift card, or payment card numbers

25 f. Content that may identify assets including bank accounts, commodities  
 26 accounts, trading accounts, personal property and/or real estate that may represent proceeds  
 27 of intrusion activity or fraud;  
 28

1           g.     Content that may reveal the current or past location of the individual or  
2 individuals using the subject accounts;

3           h.     Content that may reveal the identities of co-conspirators;

4           i.     Content that may identify any alias names, online user names, "handles"  
5 and/or "nics" of those who exercise in any way any dominion or control over the specified  
6 accounts as well as records or information that may reveal the true identities of these  
7 individuals;

8           j.     any and all other log records, including IP address captures, associated  
9 with the specified account;

10          k.     Any records or information showing the location from which the  
11 account user has accessed or utilized the accounts, including GPS, Wi-Fi, or cell tower  
12 proximity records related to the accounts;

13          l.     Any address lists or buddy/contact lists associated with the specified  
14 accounts;

15          m.     All subscriber records associated with the specified accounts, including  
16 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session  
17 times and durations; 4) length of service (including start date) and types of services utilized;  
18 5) telephone or instrument number or other subscriber number or identity, including any  
19 temporarily assigned network address such as internet protocol address, media access card  
20 addresses, or any other unique device identifiers recorded by Angelina College or Google in  
21 relation to the accounts; 6) account log files (login IP address, account activation IP  
22 addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of  
23 payment; and 9) lists of all related accounts;

24          n.     Any records of communications between Angelina College or Google  
25 and any person purporting to be the account holder about issues relating to the accounts, such  
26 as technical problems, billing inquiries, or complaints from other users about the specified  
27 account. This to include records of contacts between the subscriber and the provider's  
28 support services, as well as records of any actions taken by the provider or subscriber as a  
result of the communications.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS  
PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is \_\_\_\_\_. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Angelina College; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 EMAILS AND PROPERTY MORE FULLY  
 DESCRIBED IN ATTACHMENT A

Case No.

MI 16-472

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 1028A	Aggravated Identity Theft
Title 18, U.S.C. § 1029	Access Device Fraud
Title 18, U.S.C. § 1030	Computer Fraud

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Stacy Muldoon*  
 Applicant's signature

STACY MULDOON, SPECIAL AGENT FBI  
 Printed name and title

Sworn to before me and signed in my presence.

Date: Nov 3, 2016

City and state: SEATTLE, WASHINGTON

*Mary Alice Theiler*  
 Judge's signature

MARY ALICE THEILER U.S. MAGISTRATE JUDGE  
 Printed name and title

By *[Signature]*  
 Deputy Clerk  
 ATTEST: WILLIAM M. MCCOOL  
 Clerk, U.S. District Court  
 Western District of Washington

AFFIDAVIT

STATE OF WASHINGTON )  
 )  
 COUNTY OF KING ) ss

I, Stacy K. Muldoon, being first duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) with the FBI, currently assigned to the Seattle Field Office, and have been so employed for 12 years. I am assigned to the Cyber squad where I investigate computer intrusions. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment.

2. I make this affidavit in support of an application for a search warrant for information associated with the following accounts that are stored at a premises controlled by Angelina College, 3500 South First Street, Lufkin, Texas 75904:

**149wlong@student.angelina.edu**

**349abounds@student.angelina.edu**

**514hestes@student.angelina.edu**

The accounts to be searched are described further in the following paragraphs and in Attachment A. Angelina College has voluntarily turned over content associated with these accounts. Accordingly, this application for a warrant is sought in an abundance of caution.

Namely, this affidavit is made in support of an application for a search warrant under 18

U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Angelina College to disclose



1 to the government copies of the information, including the content of communications,  
2 further described in Section I of Attachment B. Upon receipt of the information described in  
3 Section I of Attachment B, government-authorized persons will review that information to  
4 locate the items described in Section II of Attachment B.

5 3. The facts set forth in this Affidavit are based on my own personal knowledge;  
6 knowledge obtained from other individuals during my participation in this investigation,  
7 including other law enforcement officers; review of documents and records related to this  
8 investigation; communications with others who have personal knowledge of the events and  
9 circumstances described herein; and information gained through my training and experience.  
10 Because this Affidavit is submitted for the limited purpose of establishing probable cause in  
11 support of the application for a search warrant, it does not set forth each and every fact that I  
12 or others have learned during the course of this investigation.

13 4. Based on my training and experience and the facts as set forth in this affidavit,  
14 there is probable cause to believe that violations of 18 U.S.C. § 1028A (Aggravated Identity  
15 Theft); 18 U.S.C. § 1029 (Access Device Fraud); 18 U.S.C. § 1030 (Computer Fraud); 18  
16 U.S.C. § 1349 (Conspiracy to Commit Bank and Wire Fraud) have been committed by  
17 unknown persons. There is also probable cause to search the information described in  
18 Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further  
19 described in Attachment B.

#### 20 THE INVESTIGATION

21 5. I am conducting an investigation into a data compromise affecting Eddie  
22 Bauer. Eddie Bauer identified malware running on the Windows point of sale (POS)  
23 terminals in multiple Eddie Bauer stores. The malware targeted a Java process believed to  
24 be responsible for handling communications between the standalone Verifone POS system  
25 (used to by customers and employees to "swipe" cards) and the Windows POS terminal  
26 (used by employees as registers). This malware was searching for specific details, including  
27 card numbers for credit and debit cards used to make "swipe" purchases at these POS  
28 terminals. Herein, this data will be referred to as "credit card data."

1           6.     Based on an analysis of the malware conducted by the FBI, the malware  
2 searched for and collected "Track 2" credit card data. "Track 2" credit card data is used  
3 when the credit card is "swiped" through a terminal to determine the credit card number,  
4 expiration date, and rules used to govern the transaction. If the malware detected "Track 2"  
5 data in memory, the malware would also look nearby for "Track 1" data. "Track 1" data also  
6 includes the credit card number, the expiration date, and additional information not located  
7 in "Track 2," such as the card holder's name. The malware collected and encoded the credit  
8 card data before storing the files. This encoding had the practical effect of preventing the  
9 collected data from being human readable or recognizable as credit card data

10           7.     An FBI computer scientist has conducted a preliminary examination of a  
11 version of the malware detected in Eddie Bauer's system. This preliminary examination  
12 indicates that the malware appears to be memory-resident only and was not written to the  
13 hard drive of the infected POS terminals. This is corroborated by the fact that Eddie Bauer  
14 has not yet recovered the malware on any hard drive on a compromised system. The  
15 malware was sent to the compromised system via "svchost," a built-in Windows tool, using a  
16 script designed and executed by "Powershell," another built-in Windows tool. The malware  
17 was sent from another compromised system on the Eddie Bauer network.

18           8.     Forensic investigation by Eddie Bauer shows that this activity was conducted  
19 approximately weekly by the intruders from as early as February 2016 through July 2016.  
20 Based on other forensic artifacts collected by Eddie Bauer and provided to the FBI in  
21 summary form, this activity is believed to have started on approximately January 1, 2016. It  
22 appears that every point of sale terminal, totaling approximately 1,000, was infected within  
23 the Eddie Bauer network at some point during the intruder's activity.

24           9.     Based on investigation by Eddie Bauer, as well as an investigation conducted  
25 by the FBI in a similar intrusion (see further description below), the files containing encoded  
26 stolen credit card data were then likely collected together and moved to another system  
27 within Eddie Bauer's network. Eddie Bauer recovered at least two ZIP archive files  
28 containing some of the encoded credit card data collected by the malware. There were

1 | approximately 100,000 credit card numbers located within the recovered files. Based on an  
2 | analysis of various forensic artifacts as well as transaction data kept by Eddie Bauer, Eddie  
3 | Bauer estimates roughly that as many as 2,000,000 credit and debit card numbers were  
4 | collected by the malware.

5 | 10. There is evidence of a "reverse shell" located on a test system belonging to  
6 | Eddie Bauer. Based on my training, experience, and conversation with fellow investigators I  
7 | know that a reverse shell is commonly used by intruders to connect from a compromised  
8 | system of a victim to a system under the intruder's control. This increases the likelihood that  
9 | a specific connection will bypass security measures and remain hidden because it will appear  
10 | as if the victim's computer is connecting "out" to the internet. Herein, this reverse shell will  
11 | be referred to as a "tunnel."

12 | 11. In this particular intrusion, a compromised system belonging to Eddie Bauer  
13 | connected via an encrypted tunnel to IP address 168.235.81.19, which is located in Macon,  
14 | Georgia. The suspected malware contains a persistence mechanism that – through a  
15 | scheduled Windows task – recreates the tunnel periodically to ensure that the attackers had  
16 | ongoing access to Eddie Bauer's network and systems. Eddie Bauer has seen activity as  
17 | recently as on or about July 15, 2016 on the POS terminals and also on the tunnel. Eddie  
18 | Bauer mitigated the intrusion (e.g., took steps to remove and block the malware) on or about  
19 | July 17, 2016.

20 | 12. IP address 198.199.121.106 was also accessed by a compromised  
21 | administrative account belonging to an Eddie Bauer systems administrator. This activity  
22 | involved transferring a file called "A10.zip," which likely contained stolen credit card data.

23 | 13. The Eddie Bauer system described above also accessed URL  
24 | "richardmalavet.com/images/bohs.txt" and downloaded this file. Eddie Bauer's examiners  
25 | believe that this text file contained a list of hostnames belonging to Eddie Bauer and is  
26 | believed to have been used by the intruders in furtherance of their activity on Eddie Bauer's  
27 | network. However, the file has not been recovered and analyzed yet by the FBI.

1           14. FBI Memphis is currently conducting an investigation into similar theft of  
2 credit card data from a separate business. Based on commonalities in the intruder's methods,  
3 the intrusion into Eddie Bauer and into this separate business are believed to be the work of  
4 the same individual(s). These commonalities include, but are not limited to, the following:  
5 use of the same username and nine character password to protect the tunnel into the  
6 compromised networks; the use of the same uncommon network port to send and receive  
7 communications over the tunnel; the use of the same uncommon encryption key to encode  
8 the stolen credit card data; and the use of the same file name for the malware on the point of  
9 sale system. There are some differences, however. For example, the malware employed in  
10 both schemes is slightly different in that one version of the malware appears to be an  
11 improved version of the other.

12           15. Based on tactics used in the earlier intrusion, investigators believed that the  
13 subject(s) may try to re-infect the Eddie Bauer's systems by sending a phishing email after  
14 the company performed mitigation procedures. The phishing email in the earlier intrusion  
15 originated from a specific email address, "149wlong@student.angelina.edu," and contained a  
16 Word attachment with malicious content which – when opened and activated – would re-  
17 compromised the system with malware.

18           16. Seattle FBI notified Eddie Bauer of the potential for further attacks after they  
19 mitigated. Shortly later, Eddie Bauer intercepted a phishing email that was similar to the  
20 email used in the other intrusion.

21           17. On August 5, 2016, I received a DVD from Eddie Bauer which contained the  
22 suspected phishing email that was sent to an Eddie Bauer employee.

23           18. The phishing email was sent from 149wlong@student.angelina.edu (identified  
24 within the email as an account used by "Walter Long", hereinafter referred to as "the Walter  
25 Long account") and attached a Word Document. The email stated that the sender had  
26 received "unacceptable treatment" at an Eddie Bauer store, and that the details of the  
27 incident were recorded in the attached "letter" (Microsoft Word Document) file. If the  
28 recipient of the e-mail had opened the Word Document file attached to the e-mail, they

1 would have seen a message that appears to be an instruction from Office 365 to enable  
2 macros. The only purpose of the message was to entice the viewer to enable macros so the  
3 malicious code could run. This email is consistent with the email seen in the FBI Memphis  
4 investigation, particularly with respect to the attached Word file with the malicious code.

5 19. FBI analysis of the malicious attachment sent from the Walter Long account to  
6 Eddie Bauer shows that it behaves in a similar manner as that seen in the FBI Memphis  
7 investigation. Both malicious attachments attempt to download additional malicious code  
8 from two different accounts at a free and public software repository.

9 20. According to representatives from Angelina College, the Walter Long account  
10 is illegitimate because Walter Long is not a student at the college and it is unlikely that the  
11 Walter Long account was knowingly created by individuals at Angelina College.

12 21. A representative of Angelina College provided information regarding a posting  
13 at a publically accessible website that offered to create "free .edu accounts" in exchange for  
14 compensation. The representative believes that this posting may have been made by the  
15 individual(s) who created the fraudulent Walter Long account along with two others  
16 described below. A review of the website posting described by Angelina College confirmed  
17 that there was such a posting.

18 22. In addition to this email account, representatives of Angelina College  
19 identified two additional email accounts as fraudulent and likely belonging to the same  
20 unknown individual(s). One email account was 349abounds@student.angelina.edu, which  
21 was associated with the name "Aaron Bounds" and referred to hereinafter as "the Aaron  
22 Bounds account." The second email account was 514hestes@student.angelina.edu, which  
23 was associated with the name "Henry Estes" and referred to hereinafter as "the Henry Estes  
24 account." Angelina College personnel indicated that it had previously received complaints  
25 that both the Aaron Bounds account and the Henry Estes account were involved in  
26 unspecified fraudulent activity. They also noticed during a review of the Walter Long  
27 account that all three accounts were accessed from the same IP addresses.  
28

1       23. Angelina College voluntarily provided certain records associated with the three  
2 subject accounts, including the "name" associated with each account and IP addresses used  
3 by the users of the three subject accounts to login, or access, email for the account. Angelina  
4 College voluntarily provided this information after making the determination that the  
5 accounts did not belong to actual students at the college.

6 A review of these login records by the FBI shows that on four separate occasions, at least  
7 two of these accounts were accessed from the same IP address during a very short time  
8 frame. Based on training and experience, I believe that this shows that all three accounts are  
9 under the control of the same individual or group, and that this individual or group may be  
10 using all three accounts to conduct computer intrusion activity against companies, including  
11 but not limited to Eddie Bauer and the victim in the FBI Memphis investigation. In the first  
12 instance of shared IP login behavior, the Walter Long and Aaron Bounds accounts were both  
13 accessed from the same IP address one minute apart on May 18, 2016. The Walter Long  
14 account was then accessed from this IP address again approximately 50 minutes later. The  
15 login to the Aaron Bounds account was between the two logins to the Walter Long account.  
16 This IP address is likely located in Omaha, Nebraska.

17       24. In the second instance of shared IP login behavior, the Aaron Bounds account  
18 and the Henry Estes account were both accessed from the same IP address one minute apart  
19 on May 24, 2016. The Walter Long account was accessed from this same IP address  
20 approximately three days later. This IP address is likely located in Omaha, Nebraska and is  
21 the same IP address as in the first instance of shared IP login behavior.

22       25. In the third instance of shared IP login behavior, the Walter Long and Aaron  
23 Bounds accounts were both accessed from the same IP address approximately three minutes  
24 apart on June 20, 2016. This IP address is likely located in New York, NY.

25       26. In the fourth instance of shared IP login behavior, attempted logins were made  
26 to the Henry Estes and Aaron Bounds accounts approximately one minute apart on July 8,  
27 2016. There were eight unsuccessful login attempts to the Henry Estes account over a two-  
28 minute period, followed by a successful login to the Aaron Bounds account one minute later.



1 This IP address is likely located in New York, NY but is different from the IP address seen  
2 in the third instance.

3 **THE SUBJECT ACCOUNTS ARE PERMEATED WITH FRAUD**

4 27. The government requests a warrant to search three "student" email accounts  
5 that were not set up by students and have been connected to fraudulent activity.

6 As explained above, the Walter Long account was an instrumentality of the computer  
7 intrusion. In two separate computer instructions, the account was used to convey a  
8 fraudulent consumer complaint that attached additional malware. And, employees at  
9 Angelina College report that they have connected the other two email accounts to additional  
10 fraudulent activity.

11 28. All three accounts were set up fraudulently. As explained by Angelina  
12 College, the accounts were not set up under student names; nor do they appear to have been  
13 set up by the College itself. Accordingly, the individuals who set up and used the "student"  
14 email accounts could not have had any legitimate expectation of privacy in the account they  
15 fraudulently set up using the College's email domain and services.

16 **BACKGROUND REGARDING ANGELINA COLLEGE'S SERVICES**

17 29. In my training and experience and according to information provided by  
18 Angelina College to the FBI, I have learned that Angelina College provides electronic mail  
19 ("e-mail") access to students at Angelina College. Angelina College allows students to  
20 obtain e-mail accounts at the domain name @student.angelina.edu, like the e-mail accounts  
21 listed in Attachment A. Faculty and staff at Angelina College are provided email addresses  
22 from a different domain.

23 30. According to Angelina College and publically available information, email for  
24 students at Angelina College is maintained and operated by Google, Inc. While email is  
25 minted and operated by Google Inc., personnel from Angelina College have access to the  
26 information sought by the search warrant, including IP login information and the contents of  
27 the accounts themselves.

1       31. As Angelina College is not certain how the individual(s) created the subject  
2 accounts, the exact amount of subscriber information is unknown. However, subscriber  
3 information for an Angelina College account would, based on my training and experience  
4 and information provided by Angelina College, be maintained by Google, Inc., on behalf of  
5 the college but would be accessible to college representatives.

6       32. E-mail providers typically retain certain transactional information about the  
7 creation and use of each account on their systems. This information can include the date on  
8 which the account was created, the length of service, records of log-in (i.e., session) times  
9 and durations, the types of service utilized, the status of the account (including whether the  
10 account is inactive or closed), the methods used to connect to the account (such as logging  
11 into the account via a website), and other log files that reflect usage of the account. In  
12 addition, e-mail providers often have records of the Internet Protocol address ("IP address")  
13 used to register the account and the IP addresses associated with particular logins to the  
14 account. Because every device that connects to the Internet must use an IP address, IP  
15 address information can help to identify which computers or other devices were used to  
16 access the e-mail account, which can help establish the individual or individuals who had  
17 dominion and control over the account

18       33. In general, an e-mail that is sent to an Angelina College subscriber is stored in  
19 the subscriber's "mail box" on Google, Inc.'s servers until the subscriber deletes the e-mail.  
20 If the subscriber does not delete the message, the message can remain on Google, Inc.'s  
21 servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available  
22 on Google, Inc.'s servers for a certain period of time.

23       34. When the subscriber sends an e-mail, it is initiated at the user's computer,  
24 transferred via the Internet to Google, Inc.'s servers, and then transmitted to its end  
25 destination. Google, Inc., on behalf of Angelina College, often maintains a copy of the e-  
26 mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Google, Inc.'s  
27 server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-  
28 mail, it may continue to be available on Google, Inc.'s servers for a certain period of time.

1       35. A sent or received e-mail typically includes the content of the message, source  
2 and destination addresses, the date and time at which the e-mail was sent, and the size and  
3 length of the e-mail. If an e-mail user writes a draft message but does not send it, that  
4 message may also be saved by Google, Inc. on behalf of Angelina College but may not  
5 include all of these categories of data.

6  
7                   **PAST EFFORTS TO OBTAIN THIS EVIDENCE**

8       36. This evidence has not been previously available to me or other agents. On  
9 October 5, 2016, an FBI agent sent a preservation letter to Angelina College requesting that  
10 they preserve all evidence related to the account, 149wlong@student.angelina.edu, under  
11 authority of Title 18, United States Code, Section 2703(f)(1), for a period of 90 days. In a  
12 conversation with representatives from Angelina College on October 17, 2016, they stated  
13 they had voluntarily preserved the accounts 349abounds@student.angelina.edu and  
14 514hestes@student.angelina.edu. This preservation was not requested by the FBI.

15       37. As the individual(s) utilizing these accounts are unknown to the FBI and to  
16 Angelina College, there has been no opportunity to obtain the emails sought by this search  
17 warrant via a search of the individual's computers or any other system.

18  
19                   **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

20       38. Pursuant to Title 18, United States Code, Section 2703(g), this application and  
21 affidavit for a search warrant seeks authorization to permit Angelina College, and its agents  
22 and employees, to assist agents in the execution of this warrant. Once issued, the search  
23 warrant will be presented to Angelina College with directions that it identify the Angelina  
24 College accounts described in Attachment A to this affidavit, as well as other subscriber and  
25 log records associated with the accounts, as set forth in Section I of Attachment B to this  
26 affidavit.

27       39. The search warrant will direct Angelina College to create an exact copy of the  
28 specified accounts and records.

1       40. I, and/or other law enforcement personnel will thereafter review the copy of  
2 the electronically stored data, and identify from among that content those items that come  
3 within the items identified in Section II to Attachment B, for seizure.

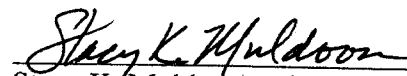
4       41. Analyzing the data contained in the forensic image may require special  
5 technical skills, equipment, and software. It could also be very time-consuming. Searching  
6 by keywords, for example, can yield thousands of "hits," each of which must then be  
7 reviewed in context by the examiner to determine whether the data is within the scope of the  
8 warrant. Merely finding a relevant "hit" does not end the review process. Keywords used  
9 originally need to be modified continuously, based on interim results. Certain file formats,  
10 moreover, do not lend themselves to keyword searches, as keywords, search text, and many  
11 common e-mail, database and spreadsheet applications do not store data as searchable text.  
12 The data may be saved, instead, in proprietary non-text format. And, as the volume of  
13 storage allotted by service providers increases, the time it takes to properly analyze  
14 recovered data increases, as well. Consistent with the foregoing, searching the recovered  
15 data for the information subject to seizure pursuant to this warrant may require a range of  
16 data analysis techniques and may take weeks or even months. All forensic analysis of the  
17 data will employ only those search protocols and methodologies reasonably designed to  
18 identify and seize the items identified in Section II of Attachment B to the warrant.

19       42. Based on my experience and training, and the experience and training of other  
20 agents with whom I have communicated, it is necessary to review and seize a variety of e-  
21 mail communications, chat logs and documents, that identify any users of the subject account  
22 and e-mails sent or received in temporal proximity to incriminating e-mails that provide  
23 context to the incriminating communications.

## 24 25 CONCLUSION

26       43. Based on the foregoing, I request that the Court issue the proposed search  
27 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of  
28 competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

1 (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has  
2 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18  
3 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or  
4 execution of this warrant. Accordingly, by this Affidavit and Warrant, I seek authority for  
5 the government to search all of the items specified in Section I, Attachment B (attached  
6 hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of  
7 the data, documents and records that are identified in Section II to that same Attachment.

8  
9 

10 Stacy K. Muldoon, Affiant  
11 Special Agent  
12 Federal Bureau of Investigation

13 SUBSCRIBED and SWORN to before me this 3 day of November 2016.

14  
15 

16 MARY ALICE THEILER  
17 United States Magistrate Judge  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A**

**Account/s to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Angelina College accounts:

**149wlong@student.angelina.edu**

**349abounds@student.angelina.edu**

**514hestes@student.angelina.edu**

As well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled by Angelina College, 3500 South First Street, Lufkin, Texas 75904.



**ATTACHMENT B**

**I. Section I - Information to be disclosed by Angelina College, for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Angelina College, including any e-mails, records, files, logs, or information that has been deleted but is still available to Angelina College, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Angelina College, is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, calendars, contact and buddy lists;

e. All records pertaining to communications between the Angelina College and any person regarding the account, including contacts with support services and records of actions taken.

**II. Section II - Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 1028A (Aggravated Identity

1 Theft), 18 U.S.C. § 1029 (Access Device Fraud); 18 U.S.C. § 1030 (Computer Fraud); and  
 2 18 U.S.C. § 1349 (Conspiracy to Commit Bank and Wire Fraud); from January 2016 to the  
 3 present , for each account or identifier listed on Attachment A, including the following:

4 a. Content that serves to identify any person who uses or accesses the  
 5 Angelina College accounts **149wlong@student.angelina.edu**,  
 6 **349abounds@student.angelina.edu**, or **514hestes@student.angelina.edu**, or who  
 exercises in any way any dominion or control over the accounts;

7 b. Content relating to the intrusion at Eddie Bauer, or communications to,  
 8 from, or about Eddie Bauer;

9 c. Content relating to attempted or successful intrusions at other victims;

10 d. Content relating to the creation, acquisition, transfer, sharing, or sale of  
 11 malicious software;

12 e. Content relating to the acquisition, transfer, sharing, sale, or disposal of  
 13 servers, email accounts, or other web services accounts used by the person or persons  
 14 conducting the Eddie Bauer intrusion or other related intrusions

15 f. Content relating to the acquisition, transfer, distribution, sharing or sale  
 16 of stolen credit card, debit card, gift card, or payment card numbers

17 g. Content that may identify assets including bank accounts, commodities  
 18 accounts, trading accounts, personal property and/or real estate that may represent proceeds  
 19 of intrusion activity or fraud;

20 h. Content that may reveal the current or past location of the individual or  
 21 individuals using the subject accounts;

22 i. Content that may reveal the identities of co-conspirators;

23 j. Content that may identify any alias names, online user names, "handles"  
 24 and/or "nics" of those who exercise in any way any dominion or control over the specified  
 25 accounts as well as records or information that may reveal the true identities of these  
 individuals;

26 k. any and all other log records, including IP address captures, associated  
 27 with the specified account;  
 28

1           l.       Any records or information showing the location from which the  
2 account user has accessed or utilized the accounts, including GPS, Wi-Fi, or cell tower  
3 proximity records related to the accounts;

4           m.       Any address lists or buddy/contact lists associated with the specified  
5 accounts;

6           n.       All subscriber records associated with the specified accounts, including  
7 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session  
8 times and durations; 4) length of service (including start date) and types of services utilized;  
9 5) telephone or instrument number or other subscriber number or identity, including any  
10 temporarily assigned network address such as internet protocol address, media access card  
11 addresses, or any other unique device identifiers recorded by Angelina College or Google in  
12 relation to the accounts; 6) account log files (login IP address, account activation IP  
13 addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of  
14 payment; and 9) lists of all related accounts;

15           o.       Any records of communications between Angelina College or Google  
16 and any person purporting to be the account holder about issues relating to the accounts, such  
17 as technical problems, billing inquiries, or complaints from other users about the specified  
18 account. This to include records of contacts between the subscriber and the provider's  
19 support services, as well as records of any actions taken by the provider or subscriber as a  
20 result of the communications.  
21  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS  
PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Angelina College, and my official title is \_\_\_\_\_. I am a custodian of records for Angelina College. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Angelina College, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Angelina College; and

c. such records were made by Angelina College as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature